|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **INSTITUTO TECNOLÓGICO DE LA PAZ**  ING.EN SISTEMAS COMPUTACIONALES | | **sistemas** | |
| **Manual de Prácticas de la Materia:**  **Seguridad en infraestructura Web** | **Unidad:**  **III** |
| **Equipo: Alfonso Delgado Aguirre,** **Jesús Fernando Inzunza Velarde** | | **Fecha: 30/10/19** | | **Grupo: H** |

|  |  |
| --- | --- |
| **No. Práctica: 2** | **Título de la Práctica: DETECCIÓN DE VULNERABILIDADES** |
| **Competencias:** | |
| **Objetivo:** Determinar los riesgos a los que están expuestos un activo informático. | |

***Marco teórico:***

**SPARTA**

Es una sencilla interfaz gráfica, escrita en Python, desarrollada para poder controlar fácilmente las funciones de las diferentes aplicaciones utilizadas generalmente desde terminal para auditar la seguridad de una red, conocer las posibles vulnerabilidades o debilidades de esta y poder enfocar nuestra protección hacia un punto concreto.

Esta herramienta nos va a permitir realizar tests de penetración en las fases de escaneo y numeración de vulnerabilidades o debilidades de los sistemas conectados a ella. De esta manera, el tiempo ahorrado en el aprendizaje y en el uso de la aplicación a nivel de terminal, puede ser utilizado para analizar los resultados que nos devolverá SPARTA, también en su propia interfaz.

**GOLISMERO**

GoLismero es una herramienta de seguridad que han presentado en la convención OWASP orientada a realizar auditorías de páginas web para buscar posibles agujeros de seguridad existentes en estas, aunque también podría ser utilizado para buscar fallos en cualquier otro tipo de servicios

***Recursos y/o Materiales:***

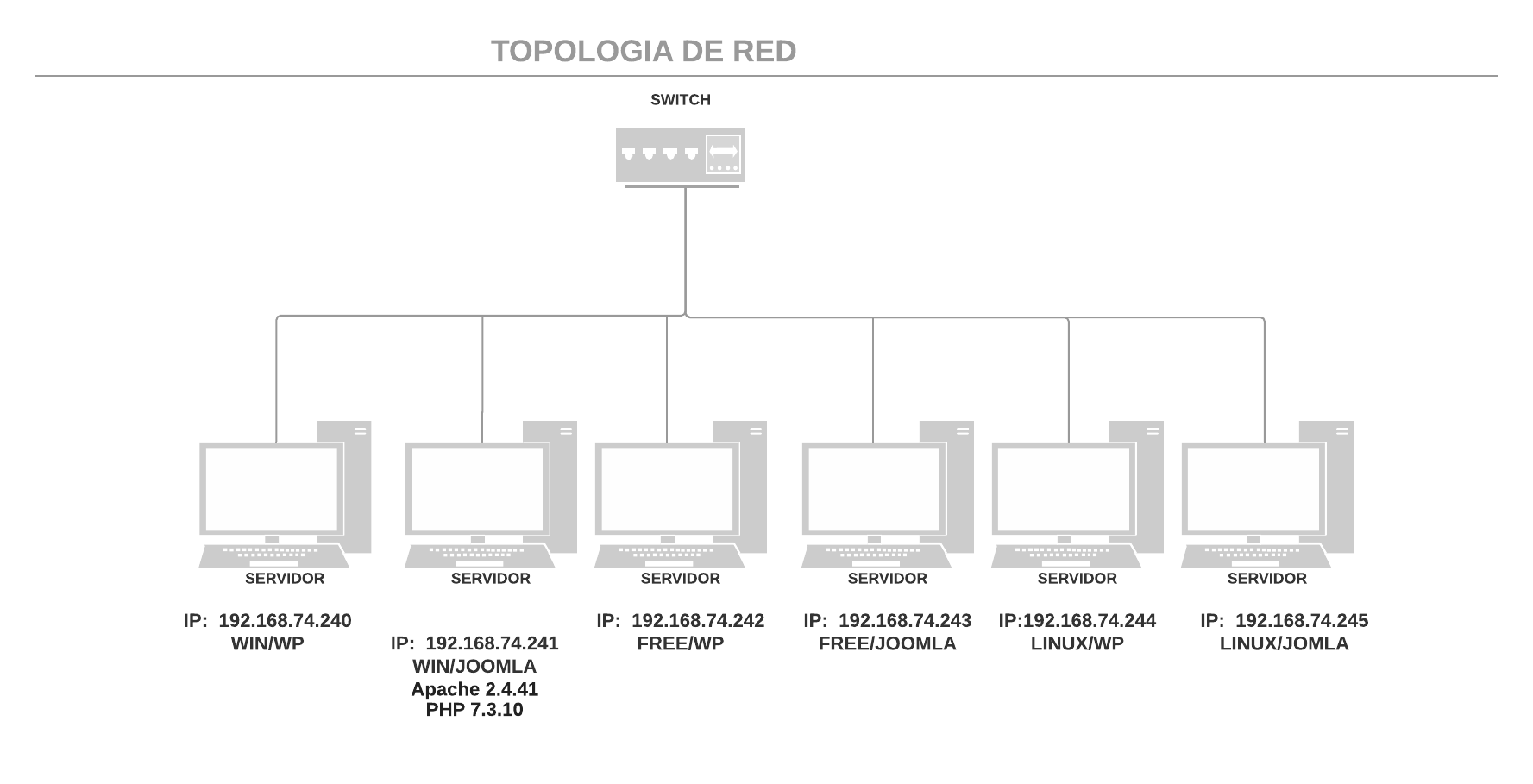
* Kali Linux
* Sparta
* Golismero
* Computadoras

***Procedimiento:***

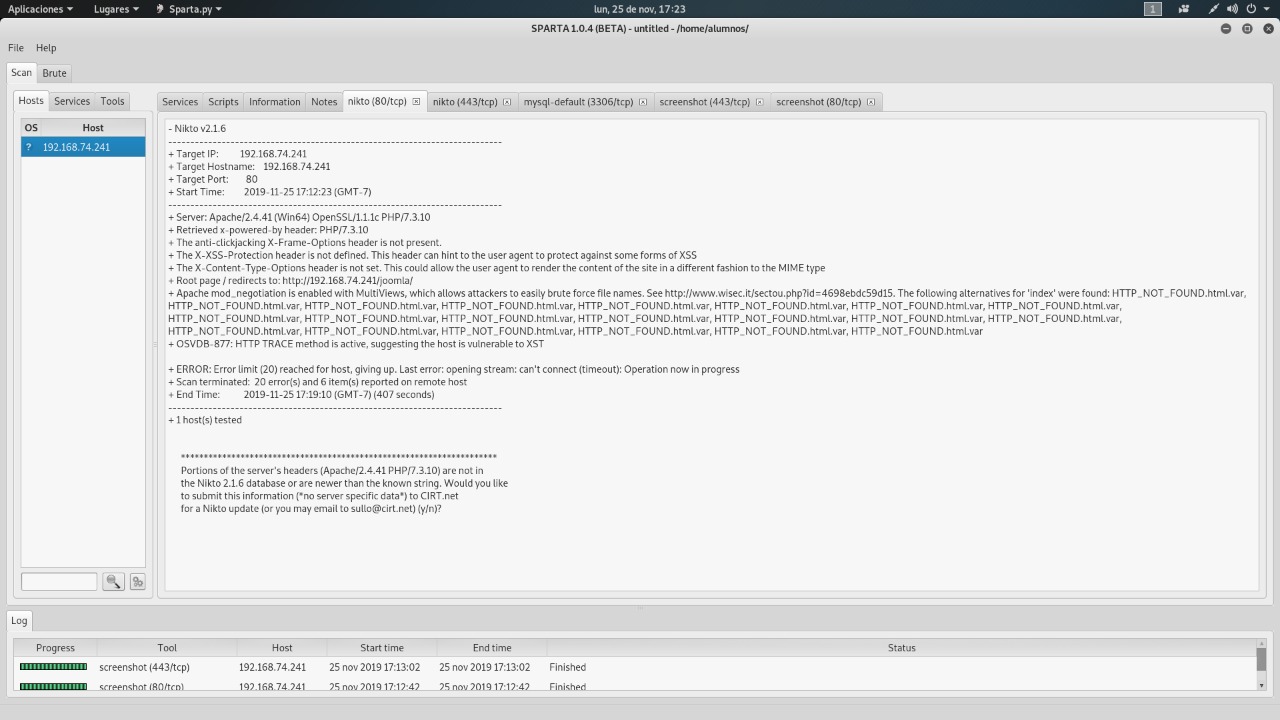
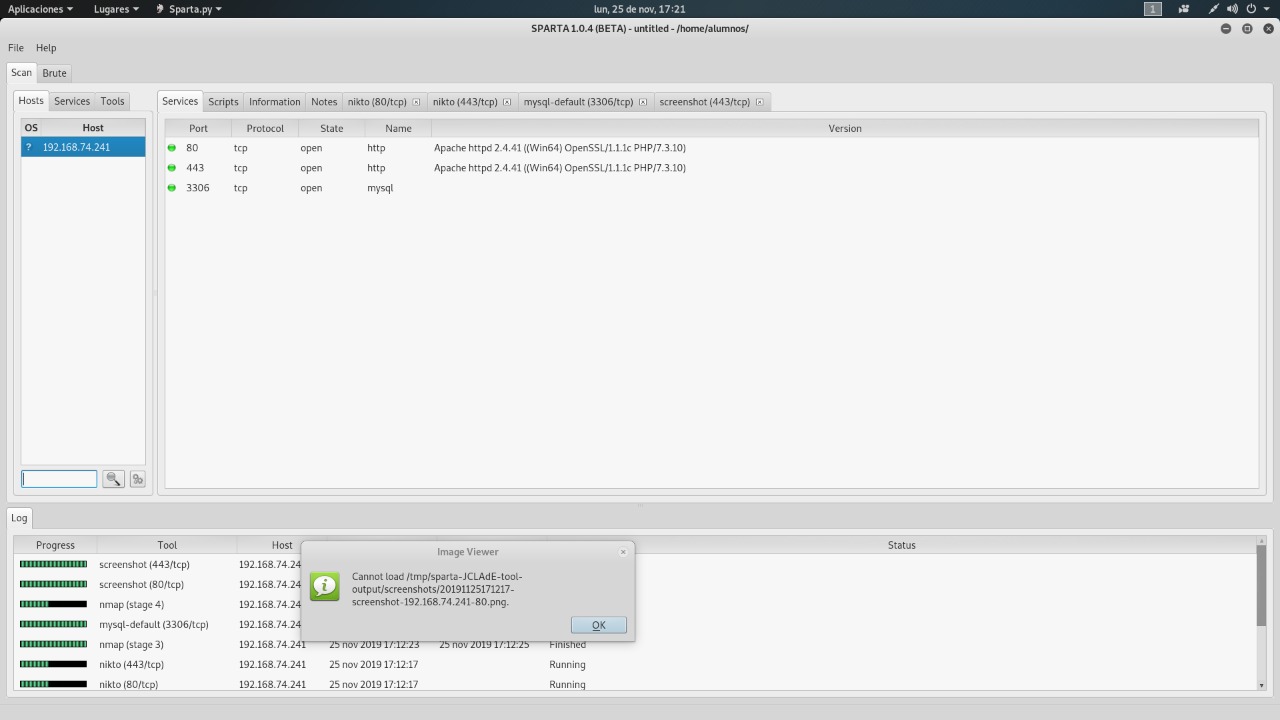
Se utiliza una herramienta de escáner de vulnerabilidades. Con el objetivo de detectar los potenciales riesgos al que están expuestos los equipos seleccionados, debido a que estos juegan el rol más crítico para la red.

***Red, IP, Topología***

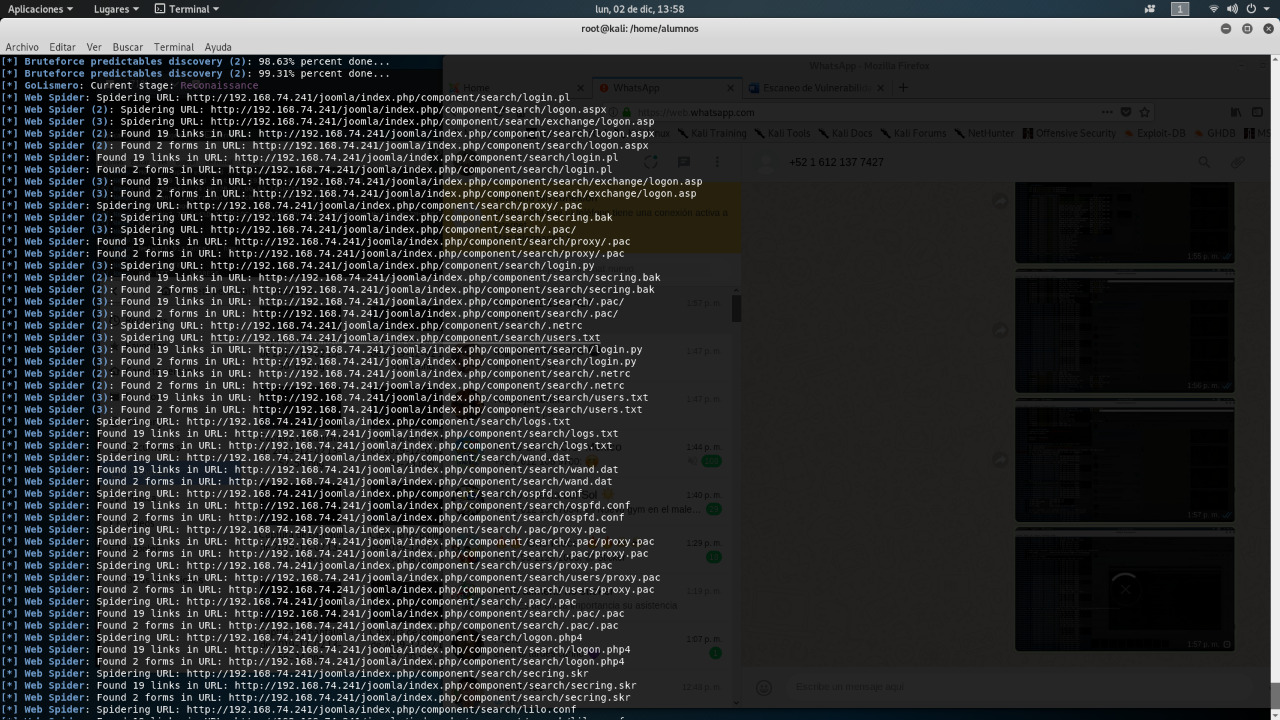
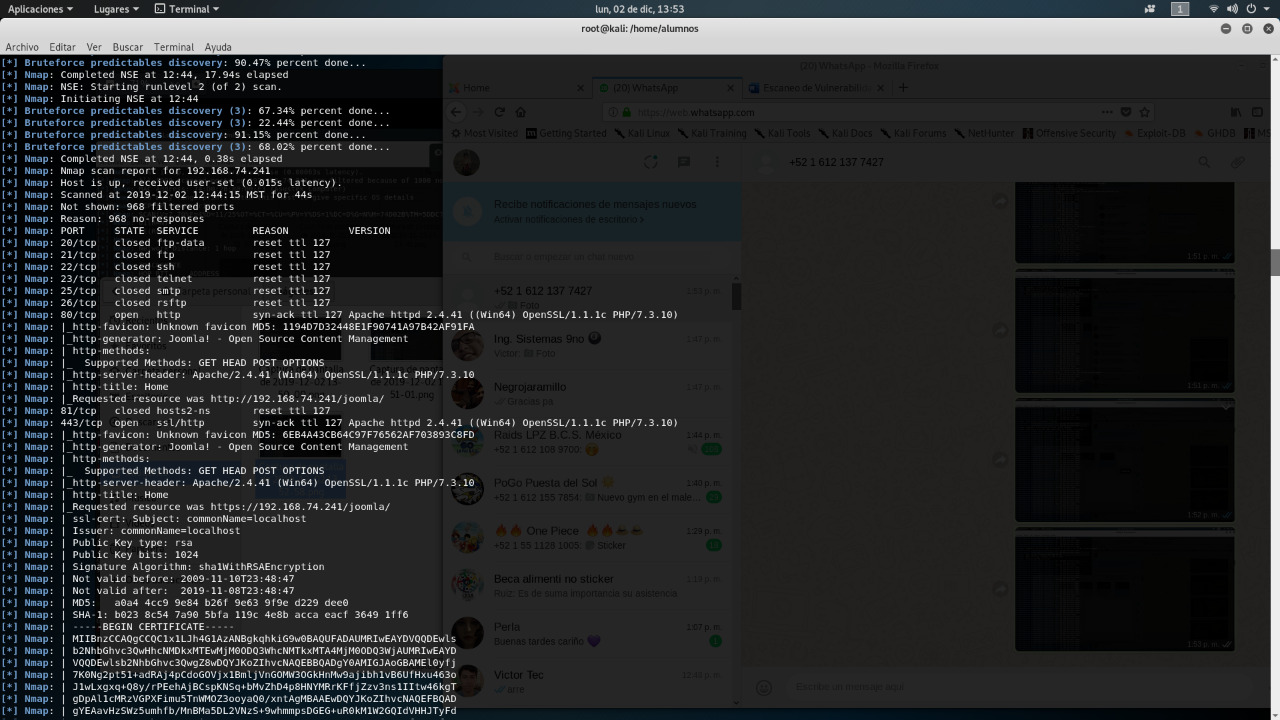
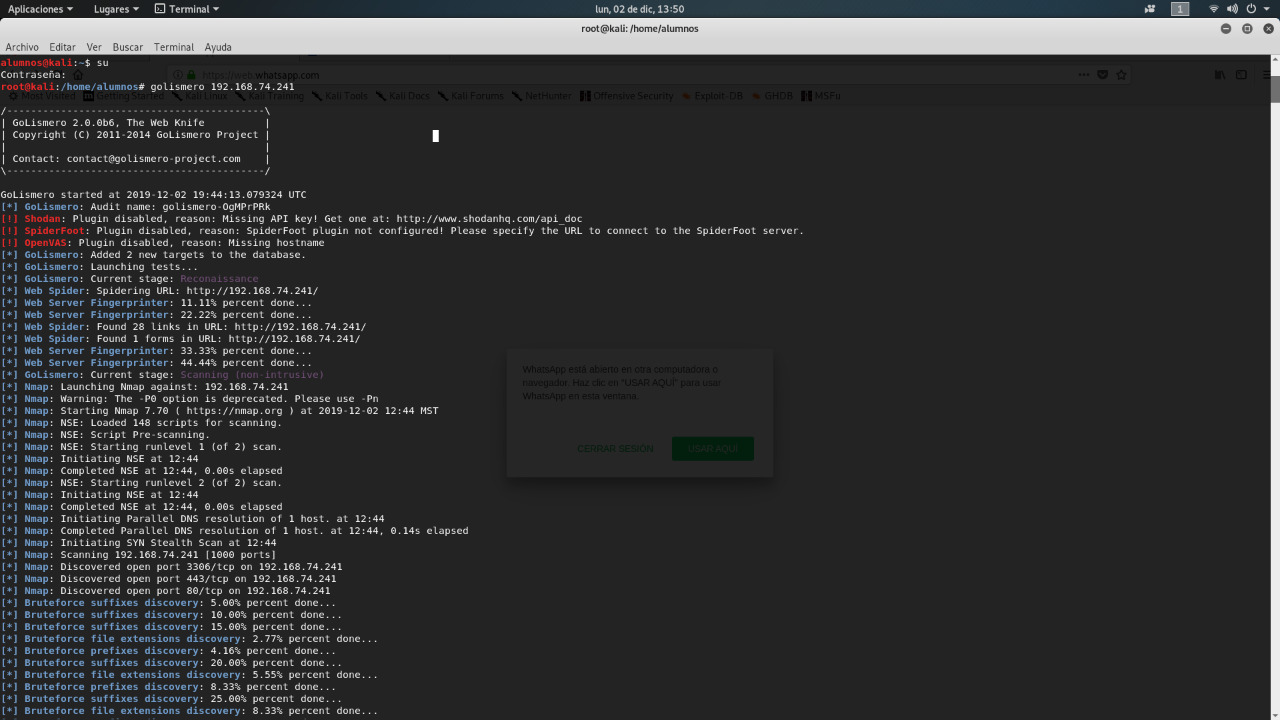
Ip servidor: 192.168.74.241



**Sparta**



**Golismero**



**EL** programa golismero no arrojo nunga vulnerabilidad, solo no arrojo información de puertos abiertos.

***Resultados:***

Con ayuda de las aplicaciones utilizadas para el análisis de vulnerabilidades detectamos las siguientes vulnerabilidades:

**Vulnerabilidades:**

* **Retrieved x-power-by header: PHP/7.3.10:**   
  x / Patrón y patrones relacionados, que permite a los atacantes remotos atacar y ejecutar código PHP arbitrario a través de un encabezado HTTP diseñado, Comandos SQL arbitrarios a través de un comentario que se maneja mal después de la recuperación de la papelera.
* **The C-XSS:** El encabezado de protección no está definido. Este encabezado lo conecta con el agente de usuario para proteger contra algunas formas de XSS.  
  Cross-site scripting (XSS) es un tipo de vulnerabilidad informática o agujero de seguridad típico de las aplicaciones Web, que puede permitir a una tercera persona inyectar en páginas web visitadas por el usuario código JavaScript o en otro lenguaje similar (ej: VBScript), se puede evitar usando medidas como CSP Política del mismo origen.  
  Es posible encontrar una vulnerabilidad de Cross-Site Scripting en aplicaciones que tengan entre sus funciones presentar la información en un navegador web u otro contenedor de páginas web. Sin embargo, no se limita a sitios web disponibles en Internet, ya que puede haber aplicaciones locales vulnerables a XSS, o incluso el navegador en sí
* **The anti-clickjacking X-Frame- Options Header is no present:**El encabezado de opciones X-Frame-anti-clickjacking no está presente. Es cuando un atacante usa múltiples capas transparentes u opacas para engañar a un usuario para que haga clic en un botón o enlace en otra página cuando tenía la intención de hacer clic en la página de nivel superior.
* **OSVDB-877:**HTTP TRACER method is active, suggesting the host is vulnerable to XST.

El método HTTP TRACER está activo, lo que sugiere que el host es vulnerable a XST.

Un ataque de rastreo entre sitios (XST) implica el uso de secuencias de comandos entre sitios (XSS) y los métodos HTTP TRACE o TRACK. Según RFC 2616 , "TRACE permite al cliente ver lo que se recibe en el otro extremo de la cadena de solicitud y usar esos datos para pruebas o información de diagnóstico", el método TRACK funciona de la misma manera pero es específico para el IIS de Microsoft Servidor web. XST podría usarse como un método para robar las cookies de los usuarios a través de Cross-site Scripting (XSS) incluso si la cookie tiene establecido el indicador " HttpOnly " y / o expone el encabezado de autorización del usuario.

***Conclusiones***

En este caso, si comparamos las herramientas que se utilizaron, podemos decir que SPARTA da más información que Golismero, que solo nos mostró procesos ejecutándose y los puertos abiertos del sitio web. Además, SPARTA fue mas entendible porque se muestra en una interfaz gráfica

***Bibliografia***